1966

Divisor Matrices in the Cayley Ring.

Charles Julius Feaux Jr
Louisiana State University and Agricultural & Mechanical College

DIVISOR MATRICES IN THE CAYLEY RING

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Charles Julius Feaux, Jr.
B.A. in Math., San Diego State College, 1958
August 1966

ACKNOWLEDGMENT

The author wishes to express his deep appreciation to Professor Gordon Pall for his constant advice, encouragement and inspiration while directing this dissertation.

TABLE OF CONTENTS

	PAGE
ACKNOWLEDGMENT	ii
ABSTRACT	iv
INTRODUCTION, NOTATION	1
CHAPTER I	4
CHAPTER II	11
BIBLIOGRAPHY	38
VITA	39

ABSTRACT

Suppose that m is an odd positive integer and that A is an integral Cayley number which is primitive mod m. The principal result of chapter 1 is

Theorem 1 If $N(A) \equiv 0(m)$, where m is odd and A is primitive mod m, then A has exactly sixteen right (left) divisors of norm m.

The sixteen divisors of A may be separated into two sets, those of one set being the negatives of those in the other set. A matrix M whose columns are the components of the divisors in one of these sets is called a divisor matrix of norm m, of A. If M is a divisor matrix and P a permutation matrix then MP is also a divisor matrix. Two divisor matrices, M_1 and M_2, norm m are called equivalent if $M_1 = M_2P$, P a permutation matrix. The main property of divisor matrices is given in

Theorem 2 Suppose M is a divisor matrix of norm m and p is any prime dividing m. Then $M'M = mI$ and M has rank four mod p.

Chapter 2 answers the following questions

1) when is the converse of theorem 2 (above) true?

2) How may right divisor matrices be distinguished from left divisor matrices? 3) what is the effect of multiplying a divisor matrix on the left by a permutation matrix?

4) How many divisors may be specified? 5) Under what conditions will two Cayley numbers, whose norms are divisible by m, have the same right (left) divisors? It is shown that every matrix, M_p, which has rank four mod p and satisfied $M_p' M_p = p^e I$ is a divisor matrix. Furthermore it is shown that a matrix can be represented in the form

$$M_p = P\begin{bmatrix} p^e I & V \\ 0 & I \end{bmatrix} U = P[V]\, U$$

where P is a permutation, $|U| = \pm 1$, and $|V| \equiv \pm 1 (p^e)$. The following theorems are then demonstrated.

Theorem 1 If M_p has the above property and if

$$M_p = P[V]\, U = Q[W]\, T$$

then $|P| \cdot |V| \equiv |Q| \cdot |W| (p^e)$. The common sign, mod p^e, is an invariant for M_p, denoted by $s(M_p)$. Question 1) and 2) are answered by

Theorem 2 If $M'M = mI$, and if M has rank four mod p for every p dividing m then there is a matrix of the type M_p such that $M_p\, U = M$. Furthermore M is a right divisor matrix if and only if all $s(M_p) = 1$. M is a left divisor matrix if and only if all $s(M_p) = -1$.

Question 3) is answered by

Theorem 3 If M is a divisor matrix of norm m define $s(M) = 1$ or -1 according as M is a right or left divisor

matrix. If P is a permutation matrix then PM is a divisor matrix and $s(PM) = |P| \cdot s(M)$. Question 4) is answered by

Theorem 4 If $N(A) \equiv N(B) \equiv 0(m)$, A and B primitive mod m, then A and B have the same set of right (left) divisors of norm m if and only if $A \equiv t\,B(m)$ for some $t \in Z$. Finally Question 5) is answered by

Theorem 5 If C_1, C_2, C_3 are linearly independent mod p, for each p dividing m, and if $(C_i, C_j) \equiv 0(m)(i,j = 1,2,3)$ then there exist A and B, $N(A) \equiv N(B) \equiv 0(m)$ such that $A\overline{C}_i \equiv \overline{C}_i B \equiv 0(m)$. If A' and B' also satisfy these congruences then $A' \equiv tA(m)$ and $B' \equiv sB(m)(s,t \in Z)$.

INTRODUCTION, NOTATION

In order to describe the ring investigated in this dissertation we first introduce the Lipschitz ring, $\mathfrak{L}$, of integral quaternions. We define $\mathfrak{L}$ as follows. Consider three symbols, i,j,k satisfying

$$i^2 = j^2 = k^2 = -1, \quad ij = k, \; jk = i, \; ki = j$$

The ring $\mathfrak{L}$ consists of all expressions of the form $X = x_0 + x_1 i + x_2 j + x_3 k$, where x_i are rational integers. $\overline{X} = x_0 - x_1 i - x_2 j - x_3 k$ is called the conjugate of X. The ring, $\mathfrak{C}$, of integral Cayley numbers is the set of all expressions of the form $A_1 + A_2 v$ with A_1 and A_2 in , where multiplication is defined by

$$(A_1 + A_2 v)(B_1 + B_2 v) = (A_1 B_1 - \overline{B}_2 A_2) + (B_2 A_1 + A_2 \overline{B}_1) v.$$

may now be described as the set of all integral linear combinations of the form

$$a_0 + a_1 i + a_2 j + a_3 k + a_4 v + a_5 iv + a_6 jv + a_7 kv$$

The expression $\overline{A} = a_0 - a_1 i - \ldots - a_7 kv = \overline{A}_1 - A_2 v$ is called the conjugate of A.

The expression $N(A) = A\overline{A} = \overline{A}A = a_0^2 + \ldots a_7^2 = N(A_1) + N(A_2)$ is called the norm of A.

We now describe some of the properties of the rings $\mathfrak{L}$ and $\mathfrak{C}$. The ring $\mathfrak{L}$ is a ring in the ordinary sense, i.e. it is associative (but not commutative). In the

ring $\mathcal{C}$ we lose not only the commutativity but associativity. There are, however, certain situations when the associative law holds. Among them are

$$\overline{A}(AB) = (\overline{A}A)\,B = (BA)\,\overline{A} = B(A\overline{A}) = N(A)\,B$$

$$A(AB) = A^2B,\quad (BA)A = BA^2$$

$(AB)(CA) = A[(BC)\,A] = [A(BC)]\,A$ (the Moufang identity)

also, $\mathcal{C}$ is an alternative algebra. That is, the expression $(AB)\,C - A(BC)$ changes sign under odd permutations of the arguments and is invariant under even permutation of the arguments.

If $A = a_0 + \ldots + a_7 kv$ and $B = b_0 + \ldots + b_7\,kv$ then the expression

$(A,B) = a_0\,b_0 + \ldots + a_7\,b_7 = 1/2\,\{N(A + B) - N(A) - N(B)\}$

enjoys the following properties. It is a symmetric bilinear form in the coefficients of A and B. We also have $(A,A) = N(A)$, $(A,BC) = (A\overline{C},B) = (\overline{B}A,C)$, $(AB,CB) = (A,C)\,N(B)$ If $(A,B) = 0$ A and B will be called orthogonal. These and other facts may be found in [2].

Given a positive integer n we will write $A \equiv B \bmod n$, or $A \equiv B(n)$, if $a_i \equiv b_i(n)(i = 0, \ldots, 7)$. This is a congruence relation with respect to addition and multiplication. We also have $(A_1,B_1) \equiv (A_2,B_2)(n)$ and $N(A_1) \equiv N(A_2)(n)$, if $A_1 \equiv A_2(n)$ and $B_1 \equiv B_2(n)$. A will be called primitive, mod n, if its components are prime

to n. If $A \in \mathfrak{C}$, or if $\mathfrak{V} \subset \mathfrak{C}$, the symbol A_n, or $\mathfrak{V}_n$, will denote the residue class determined by A, or the residue classes determined by the elements of $\mathfrak{V}$, mod n. $\mathfrak{C}_p$ (or $\mathfrak{L}_p$) may be regarded as vector spaces over the field $Z/(p)$ (Z = the ring of rational integers). If $X_1, \ldots, X_n$ are in $\mathfrak{C}$, the symbol $(X_1, \ldots, X_n)_p$ means the space generated by the integral linear combinations of $X_1, \ldots, X_n$ mod p. A set $\mathfrak{V}_p$, $\mathfrak{V} \subset \mathfrak{C}$, is called isotropic if $N(X) \equiv 0(p)$ for every X in $\mathfrak{V}$. In chapter 2 we will use the following fact. Let $(X_1, \ldots, X_n)_p$ be a subspace of $\mathfrak{C}_p$, with basis $X_1, \ldots, X_n$, mod p, which is isotropic. Then $\mathfrak{C}_p$ contains a subspace of the type $(X_1, Y_1)_p \perp \cdots \perp (X_n, Y_n)_p$ where $(X_i, Y_i) \not\equiv 0(p) (i = 1, \ldots, n)$. $\perp$ stands for an orthogonal direct sum. This last statement implies that $n \leq 4$. This fact may be found in [1].

Unless otherwise specified capital Latin letters will denote elements of $\mathfrak{C}$ while small Latin letters will denote elements of Z. The letter p will always denote an odd prime. The symbols R(A,p), L(A,p), R'(A,p), L'(A,p) will stand for the vector spaces $\{XA \mid X \in \mathfrak{C}\}_p$, $\{AX \mid X \in \mathfrak{C}\}_p$, $\{X \mid XA \equiv 0(p)\}_p$, $\{X \mid AX \equiv 0(p)\}_p$ respectively.

CHAPTER I

We begin this chapter by proving

Theorem 1 Let $X = x_0 + x_1 i + \ldots + x_1 kv$ and let m be an odd positive integer with $1 = (m, x_0, \ldots, x_7)$. If $N(X) \equiv 0(m)$ then X has exactly sixteen right divisors of norm m and exactly sixteen left divisors of norm m.

The proof which we give here is due to Pall and Todd, and will appear in a paper soon to be published. The theorem is proved in several steps. In what follows, m and X will have the properties described in theorem 1. Some of the lemmas which are stated follows by means of relatively simple calculations. Hence their proofs will be omitted.

Lemma 1 The linear mapping induced on $\mathfrak{C}$ by $1 \to 1$, $i \to j$, $j \to iv$, $k \to kv$, $v \to i$, $iv \to -k$, $v \to v$, $kv \to jv$ is a norm preserving automorphism which will be denoted by σ. Furthermore, σ has order seven and each power of σ has determinant 1.

Lemma 2 Consider $X = x_0 + \ldots + x_7 kv = X_1 + X_2 v$ $(X_i \in \mathfrak{C})$. Suppose $N(X) \equiv 0(p)$ and $(p, x_0, \ldots, x_7) = 1$. If $N(X_1) \equiv 0(p)$ then we can find an automorphism $\emptyset$, from lemma 1, such that $\emptyset(X) = Y_1 + Y_2 v$ $(Y_i \in \mathfrak{C})$ has $N(Y_1) \not\equiv 0(p)$.

Proof Abbreviate $x_r^2 + x_s^2$ as (rs) and $x_r^2 + x_s^2 + x_t^2 + x_u^2$ by (rstu). If p divides (0123), (0145), (0167) then (on adding) p divides (01). Similarly p divides (02) and (03). Hence (on adding) p divides x_0, x_1, x_2, x_3. Also p divides (45), (46), and (47) hence x_4, x_5, x_6, x_7.

Lemma 3 Let $X = X_1 + X_2 v$ ($X_i \in \mathfrak{L}$). Then the number of ordered pairs Y, Z satisfying

1) $$X = ZY \quad , \quad N(Y) = m$$

1') $$X = YZ \quad , \quad N(Y) = m$$

is equal to the number of elements Y such that $X\overline{Y} \equiv 0(m)$ with $N(Y) = m$ and hence is equal to the number of pairs Y_1, Y_2 ($Y_i \in \mathfrak{L}$) satisfying

2) $$X_1 \overline{Y}_1 + \overline{Y}_2 X_2 \equiv 0, \quad X_2 Y_1 - Y_2 X_1 \equiv 0 \quad (m)$$

3) $$\overline{Y}_1 Y_1 + \overline{Y}_2 Y_2 = m$$

Completely analogous statements hold for Y on the left if the congruences 2) are replaced by

2)' $$\overline{Y}_1 X_1 + \overline{X}_2 Y_2 \equiv 0, \quad X_2 \overline{Y}_1 - Y_2 \overline{X}_1 \equiv 0(m)$$

Lemma 4 Let p^e divide $N(X)$ and assume $N(X_1)$ (hence $N(X_2)$) prime to p. Then each of the congruences in 2) is equivalent to the single condition.

4) $$N(X_1) Y_1 \equiv - \overline{X}_2 Y_2 X_1 (p^e)$$

For Y on the left we have

4)' $$N(X_1)\ Y_1 \equiv \overline{X}_1\ \overline{Y}_2\ X_2(p^e)$$

Lemma 5 Set $W_1 = w_0 + w_1 i + w_2 j + w_3 k$ and $W_2 = w_4 + w_5 i + w_6 j + w_7 k$, and assume the hypotheses of lemma 4. Choose h such that $hN(X_1) \equiv 1(p^e)$. Then every solution of 4), or 4)', is comprised in the formula

5) $$Y_2 = W_2,\ Y_1 = -\ h\overline{X}_2\ W_2\ X_1 + p^e W_1$$

or

5)' $$Y_2 = W_2,\quad Y = -\ h\overline{X}_1\ \overline{W}_2\ X_2 + p^e W_1$$

for arbitrary W_1, W_2 in $\mathfrak{L}$. Hence 4) and 4)' are expressed by the following integral linear substitutions of determinant p^{4e} on the components $y_0, \ldots, y_7$ of Y:

6) $$(y_0, \ldots, y_7)' = \begin{bmatrix} p^e I & V \\ 0 & I \end{bmatrix} (w_0, \ldots, w_7)'$$

Lemma 8 Let S and T be integral square matrices of the same order k, with coprine determinants s,t. Then there exists a square matrix N of determinant st such that $N = SK = TL$, where K and L are integral matrices of order k.

Proof See lemma 6, page 354, of [4].

Lemma 9 In lemma 8, let α denote an integral matrix with k rows and one column. Then $S^{-1}\alpha$ and $T^{-1}\alpha$ are integral

if and only if $N^{-1}\alpha$ is integral.

Proof If $S^{-1}\alpha$ is integral then $K^{-1}S^{-1}\alpha$ is integral mod s. If $T^{-1}\alpha$ is integral then $L^{-1}T^{-1}\alpha$ is integral mod t. Since $(s,t) = 1$, $N^{-1}\alpha$ is integral. Conversely, if $N^{-1}\alpha$ is integral then $S^{-1}\alpha = K(N^{-1}\alpha)$ is integral.

We are now in a position to prove theorem 1. If p divides m and $N(X_1) \equiv 0(p)$ then we may apply one of the automorphisms of lemma 1 to secure $N(X_1) \not\equiv 0(p)$. Hence for each p^e in m there is an integral matrix S_p of determinant p^{4r} such that, if α denotes the column vector with the same components y_i as Y, $X\overline{Y} \equiv 0(p^e)$ if and only if $S_p^{-1}\alpha$ is integral. By lemmas 8 and 9 there is an integral matrix N of determinant m^4 such that $X\overline{Y} \equiv 0(p^e)$ for each p in m if and only if $N^{-1}\alpha$ is integral, i.e. $\alpha = N\zeta$ with ζ integral. The transformation $\alpha = N\zeta$ replaces. $N(Y) = y_0^2 = \ldots = y_7^2$ by a form $\Sigma b_{ij}w_iw_j$. For arbitrary integers $w_0, \ldots, w_7$ the numbers $y_0, \ldots, y_2$ given by $\alpha = N\zeta$ satisfied $X\overline{Y} \equiv 0(m)$, hence $(X\overline{Y})Y \equiv 0$ or $X(y_0^2 + \ldots + y_7^2) \equiv 0(m)$. But X is primitive mod m. Hence $\Sigma\, b_{ij}\, w_i\, w_j$ is an integer divisible by the odd integer m, for any integers $w_0, \ldots, w_7$. Hence by a familiar argument (take one or two of the w_i equal to 1, the rest 0), $b_{ij} = mc_{ij}$, and the number of factorizations

(1) equals the number of representations of 1 by the form

$\Sigma\, c_{ij}\, w_i w_j$ in integers $w_0, \ldots, w_7$. But $\Sigma\, c_{ij} w_i w_j$ has been derived from $\Sigma\, y_i^2$ by an integral transformation of determinant m^4, and then cancelling m. Hence $\Sigma\, c_{ij} w_i w_j$ is positive definite and of determinant $1 \cdot (m^4)^2/m^8 = 1$. Setting $Y = X$ if $N(X)$ is odd or $Y = X + m$ if $N(X)$ is even we obtain Y such that $X\overline{Y} \equiv O(m)$ with $N(Y)$ odd. Hence $\zeta = N^{-1}\alpha$ is integral and $\Sigma\, c_{ij} w_i w_j = \frac{1}{m} \Sigma\, y_i^2$ is odd. Since $\Sigma\, c_{ij} w_i w_j$ is positive definite, of determinant 1, and represents odd numbers we know it is in the class of $\Sigma\, t_i^2$. See [3]. A similar argument holds for Y on the left.

In the proof of theorem 1 the form $\Sigma\, y_i^2$ was transformed into the form $m\, \Sigma\, c_{ij} w_i w_j$ by the transformation $\alpha = N\zeta$. Let τ denote the column matrix with components $t_0, \ldots, t_1$. Then there is a unimodular matrix U such that $\zeta = U\tau$ transforms $\Sigma\, c_{ij} w_i w_j$ into $\Sigma\, t_i^2$. If $M = NU$ then the transformation $\alpha = M\tau$ carries $\Sigma\, y_i^2$ into $m\, \Sigma\, t_i^2$. This says that $M'IM = mI$. Also, it is easy to see that the components of the divisors of X are the columns of M together with their negatives. Hence if P is any permutation matrix of order eight the columns of the matrix MP are components of divisors of X of norm m. Such a matrix is called a divisor matrix of

norm m. We define two such matrices, M_1 and M_2, to be equivalent if $M_1 = M_2P$ for some permutation P.

We now look more closely at the matrices from which N was composed. By applying a suitable automorphism to ζ some permutation of $(y_0, \ldots, y_7)'$ is expressable in the form 6). By applying the universe of this automorphism we obtain

$$6)' \qquad (y_0, \ldots, y_7)' = S \begin{bmatrix} p^e I & V \\ 0 & I \end{bmatrix} (w_0, \ldots, w_7)'$$

Hence

$$7) \qquad M = S \begin{bmatrix} p^e I & V \\ 0 & I \end{bmatrix} K$$

where $|K|$ is prime to p. From this we see that M has rank four mod p. We also note that

$$\begin{bmatrix} p^e I & 0 \\ V' & I \end{bmatrix} \begin{bmatrix} p^e I & V \\ 0 & I \end{bmatrix} = \begin{bmatrix} p^{2e} I & p^e V \\ p^e V' & V'V + I \end{bmatrix} \equiv 0(p^e)$$

Thus $V'V \equiv -I(p^e)$ and $|V| \equiv \pm 1(p^e)$. We collect some of the above remarks in

Theorem 2 If M is a divisor matrix then M has rank four mod p and satisfies $M'M = mI$.

We are now able to raise the following questions

1) Is the converse of theorem 2 true?

2) How many divisors may be specified?

3) Under what conditions will two Cayley numbers, of norm divisible by m; have the same right (left divisors of norm m?

4) How may we distinguish right divisor matrices from left divisor matrices?

5) What is the effect of multiplying M on the left by a permutation matrix.

We will answer question 11 in the affirmative. We will show that three Cayley numbers C_1, C_2, C_3 which are linearly independent mod p (for each p in m) and which satisfy $(c_{ij}\ c_j) = \delta_{ij} m$ $(i,j = 1,2,3)$ can be right (left) divisors of norm m of a uniquely determined Cayley number. Furthermore A and B have the same right (left) divisors of norm m if and only if $A \equiv tB(m)$ for some t.

Questions 4) and 5) will be answered by means of the sign of $|V|$ in equation 7).

CHAPTER II

In this chapter a sequence of lemmas will be proved which will enable us to establish the statements made at the end of the last chapter. We begin with

Lemma 1 If $N(A) \equiv 0$, but $A \equiv O(p)$, then each of the vector spaces $R(A,p)$, $L(A,p)$, $R'A,p)$, $L'A,p)$ is of dimension four. Furthermore if $N(A) \equiv O(p^r)$ then $XA \equiv O(p^r)$ if and only if $X \equiv Y\overline{A}(p^r)$ for some Y and $AX \equiv O(p^r)$ if and only if $X \equiv \overline{A}Y(p^r)$ for some Y.

Proof Let $A = A_1 + A_2v$, $A_i \in \mathfrak{L}$. We will reduce the problem of proving that dim $R(A,p) = 4$ to the case where $N(A_1) \not\equiv O(p)$. For, if $N(A_1) \equiv O(p)$, then by lemma 2 of chapter 1 there exists an automorphism of $\mathfrak{C}$ which carries A into an element $B = B_1 + B_2v$, $B_i \in \mathfrak{L}$, of $\mathfrak{C}$ with $N(B_1) \not\equiv O(p)$. This automorphism induces an automorphism on $\mathfrak{C}_p$ which carries $R(A,p)$ onto $R(B,p)$. Now if $X \in \mathfrak{L}$ the map $X \to XA$ induces an isomorphism of the vector space $\mathfrak{L}_p$ into the vector space $\mathfrak{C}_p$, for $XA \equiv XA_1 + (A_2X)v \equiv O(p)$ implies $XA_1 \equiv O(p)$ which implies $X \equiv O(p)$. Therefore dim $R(A,p) \geq 4$ and since $R(A,p)$ is isotropic dim $R(A,p) \leq 4$. The map which $X \to XA$ induces on $\mathfrak{C}_p$ has $R'(A,p)$ as its kernel and this implies that dim $R'(A,p) = 4$. Since $(X\overline{A})\,A \equiv O(p)$ we have $R(\overline{A},p) \subset R'(A,p)$ and therefore $R(\overline{A},p) = R'(A,p)$ because the dimensions of the two spaces are equal. This means that $XA \equiv O(p)$ if and only if

$X \equiv Y\overline{A}(p)$ for some Y. If now $N(A) \equiv O(p^{r+1})$ and $XA \equiv O(p^{r+1})$ then $X \equiv Y\overline{A}(p^r)$ (by induction) and therefore $X \equiv Y\overline{A} + p^r Z(p^{r+1})$. Upon multiplying through by A we have $ZA \equiv O(p)$ and thus $Z \equiv T\overline{A}(p)$ or $p^r Z \equiv p^r T\overline{A}(p^{r+1})$ which gives $X \equiv (Y + p^r T)\,\overline{A}\,(p^{r+1})$. The results for A on the left follow by noting that $X \to \overline{X}$ induces an automorphism of the vector space ζ_p taking $R(\overline{A},p)$ onto $L(A,p)$ and $R'(\overline{A},p)$ onto $L'(A,p)$.

Note: We have also shown that if $N(A) \equiv O(p)$ and $A = A_1 + A_2 v$ with $N(A_1) \not\equiv (p)$, $A_i \in \mathcal{L}$, then given Y there exists a uniquely determined element X of $\mathcal{L}$ such that $XA \equiv YA(p)$ or $AX \equiv AY(p)$. Furthermore if $N(A) \not\equiv O(p)$ then dim $R(A,p)$ = dim $L(A,p)$ = 8 and dim $R'(A,p)$ = dim $L'(A,p)$ = 0 since the map $X \to XA$ is then an automorphism mod p.

Lemma 2 If $N(A) \equiv N(B) \equiv O(p)$, but $A \not\equiv 0 \not\equiv B(p)$, then

$$\dim R(A,p) \cap R(B,p) = \begin{cases} 4 \text{ if } B \equiv t\,A(p) \\ 2 \text{ if } (A,B) \equiv O(p) \text{ but } B \not\equiv tA(p) \text{ for any } t \\ 0 \text{ if } (A,B) \not\equiv O(p) \end{cases}$$

The same conclusions follow for dim $L(A,p) \cap L(B,p)$.

Proof Let $A = A_1 + A_2 v$ and $B = B_1 + B_2 v$, A_i and $B_i \in \mathcal{L}$. We first assume that $N(A_1) \not\equiv 0 \not\equiv N(B_1)$ (p). Now $C_p \in R(A,p) \cap R(B,p)$ if and only if there exist, by the above note, elements X and Y of $\mathcal{L}$ such that

$XA \equiv YB \equiv C(p)$. The first congruence is equivalent to $XA_1 \equiv YB_1(p)$ and $A_2X \equiv B_2Y(p)$. If $N(A_1)h \equiv 1(p)$ then the above two congruences are equivalent to $X \equiv -h\,\overline{A}_2B_2Y(p)$ and $X \equiv h\,Y\,B_1\overline{A}_1(p)$. Hence there is $C \not\equiv 0(p)$ such that $C_p \in R(A,p) \cap R(B,p)$ if and only if there exists Y in $\mathcal{L}$, $Y \not\equiv 0(p)$, such that $(-\overline{A}_2B_2)\,Y \equiv Y(B_1\overline{A}_1)(p)$. The number of linearly independent solutions of this congruence is, therefore, the dimension in question. Notice that $N(-\overline{A}_2B_2) \equiv N(B_1\overline{A}_1) \not\equiv 0(p)$ since $N(A_1) \equiv -N(A_2)$ mod p and $N(B_1) \equiv -N(B_2)(p)$.

We now determine conditions under which the congruence $A'Y \equiv YB'(p)$ is solvable for $Y \in \mathcal{L}$ where A' and B' are given elements of $\mathcal{L}$ with $N(A') \equiv N(B') \not\equiv 0(p)$. If $A' = a_0 + a_1i + a_2j + a_3k$, $B' = b_0 + b_1i + b_2j + b_3k$ then a simple calculation shows that the coefficient matrix of $A'Y - YB' \equiv 0(p)$ is:

$$\begin{matrix} a_0 - b_0 & -a_1 + b_1 & -a_2 + b_2 & -a_3 + b_3 \\ a_1 - b_1 & a_0 - b_0 & -a_3 - b_3 & a_2 + b_2 \\ a_2 - b_2 & a_3 + b_3 & a_0 - b_0 & -a_1 - b_1 \\ a_3 - b_3 & -a_2 - b_2 & a_1 + b_1 & a_0 - b_0 \end{matrix}$$

The determinant of the above matrix is:

$$(N(B') - N(A'))^2 + 2(a_0^2 - b_0^2)(N(B') - N(A')) + 2\,(a_0 - b_0)^2(N(B') + N(A'))$$

which is congruent to $4N(A')\ (a_0 - b_0)^2\ (p)$ since $N(A') \equiv N(B')$ mod p. Thus our congruence has a solution if and only if $a_0 \equiv b_0(p)$. The solution space has dimension four if and only if $a_0 \equiv b_0$, $a_i \equiv b_i(p)$, and $a_i \equiv -b_i(p)$ $(i = 1,2,3)$. This is equivalent to $a_0 \equiv b_0(p)$ and $a_i \equiv b_i \equiv 0(p)$ which is in turn equivalent to $A' \equiv B' \equiv t(p)$ for some t. If the rank of the coefficient matrix is neither zero nor four it is then a non zero skew symmetric matrix of determinant zero and by elementary row and column operations it is easy to see that the rank is then two. We have shown that the dimension of the solution space of $A'Y - YB' \equiv 0(p)$ is 4, 2, or 0 according as $A' \equiv B' \equiv t(p)$, A' and B' are not linearly independent mod p but $a_0 \equiv b_0(p)$ or $a_0 \not\equiv b_0(p)$ respectively.

Returning to the original congruence we set $A' = -\bar{A}_2\ B_2$ and $B' = B_1\ \bar{A}_1$. Now $a_0 \equiv b_0(p)$ if and only if $(-\bar{A}_2\ B_2,\ 1) \equiv (B_1\ \bar{A}_1,\ 1)\ (p)$ or $(A_2,\ B_2) + (A_1,\ B_1) = (A,\ B) \equiv 0(p)$. $A' \equiv B' \equiv t(p)$ if and only if $-\bar{A}_2\ B_2 \equiv t(p)$ and $B_1\ \bar{A}_1 \equiv t(p)$ or $B_2 \equiv h\ t\ A_2(p)$ and $B_1 \equiv h\ t\ A_1(p)$ which is $B \equiv (ht)A(p)$.

We now supose that $N(A_1) \not\equiv 0(p)$ and $N(B_1) \equiv 0(p)$. In this case $N(B_1 - tA_1) = -2t(A_1,\ B_1) + t^2\ N(A_1)$. Thus one may find $t \in Z$ so that $N(B_1 - tA_1) \not\equiv 0(p)$. If we set $B' = B - tA$ then $B' \not\equiv 0(p)$, since $B \equiv tA(p)$ and $B \not\equiv 0(p)$ imply that $N(B_1) \not\equiv 0(p)$. Also $N(B_1') \not\equiv 0(p)$.

Regardless of whether $N(B') \equiv 0(p)$ or $N(B') \not\equiv 0(p)$ the criteria stated in the lemma are invariant when B is replaced by B'. Since $(A,B') = (A,B - tA) = (A,B) - t(A,A) \equiv (A,B)\ (p)$ and $B \equiv aA(p)$ $B' \equiv a'A(r)$ are both impossible for any a and a' since $B \not\equiv 0(p)$, $B' \not\equiv 0(p)$ and $N(B_1) \not\equiv 0(p)$. Consider now the spaces $R(A,p)$, $R(B,p)$ and $R(B',p)$. From the equations

$$XA + YB = (X + tY)\ A + YB'$$

and

$$XA + YB' = (X - tY)A + YB$$

it follows that

$$R(A,p) + R(B',p) = R(A,p) + R(B,p).$$

We now have the two equations:

$$\dim (R(A,p) + R(B',p)) = \dim R(A,p) + \dim R(B',p) - \dim (R(A,p) \cap R(B',p))$$

and

$$\dim(R(A,p) + R(B,p)) = \dim R(A,p) + \dim(B,p) - \dim(R(A,p) \cap R(B,p))$$

We now take the two cases $N(B') \not\equiv 0(p)$ and $N(B') \equiv 0\,(p)$. If $N(B') \not\equiv 0(p)$ then, by the note at the end of lemma 1, the above equations, and the fact that

$$R(A,p) + R(B,p) = R(A,p) + R(B',p)$$

we have $\dim (R(A,p) \cap R(B',p)) = \dim (R(A,p) \cap R(B,p)) = 0$. But if $N(B') = N(B - tA) = -2t\,(A,B) \not\equiv 0(p)$ we have $(A,B) \not\equiv 0(p)$. If on the other hand $N(B') \equiv 0(p)$ then we

have $(A,B) \equiv (A,B') \equiv 0(p)$. But in this case we also have: $\dim (R(A,p) \cap R(B,p)) = \dim (R(A,p) \cap R(B',p)) = 2$. Since B' now satisfies the conditions of the lemma for the case already proved and since A and B as well as A and B' are linearly independent mod p the lemma is established in this case.

Finally if $N(A_1) \equiv N(B_1) \equiv 0(p)$ we may secure $N(A_1) \not\equiv 0(p)$ by an automorphism (lemma 1, chapter 1) of ζ_p. Since norms inner products, primitivity, and the dimensions of vector space are unaltered the lemma is proved.

The lemma is proved for $L(A,p)$ and $L(B,p)$ by considering the map that $X \to \overline{X}$ induces on the vector space ζ_p. For under this map $R(\overline{A},p)$ is carried onto $L(A,p)$ and $R(\overline{B},p)$ is carried onto $L(B,p)$, as in lemma 1, and $(A,B) = (\overline{A},\overline{B})$ as well as $A \equiv tB(p)$ if and only if $\overline{A} \equiv t\overline{B}(p)$.

Lemma 3 If C_1, C_2, C_3 are linearly independent mod p and satisfy $(C_i, C_j) \equiv 0(p)$ $(i,j = 1,2,3)$ then there exist A_1 and A_2 primitive mod p such that $A_1\overline{C}_i \equiv 0(p)$ and $\overline{C}_i A_2 \equiv 0(p)$ $(i = 1,2,3)$. If B_1 and B_2 also satisfy these congruences and are primitive mod p then $B_k \equiv t_k A_k(p)$ for some t_k $(k = 1,2)$.

Proof We will prove that there exists an A such that $A\overline{C}_i \equiv 0(p)$, and that $B\overline{C}_i \equiv 0(p)$ implies $B \equiv tA(p)$. The other result will then follow by taking conjugates.

Consider the spaces $R(C_i,p)$ $(i = 1,2,3)$ It will be shown that

$$\dim R(C_1,p) \cap R(C_2,p) \cap R(C_3p) = 1$$

Since $(C_i, C_j) \equiv 0(p)$, but $C_i \not\equiv tC_j(p)$ for any $t(i \neq j)$, it follows by lemma 2 that dim $R(C_ip) \cap R(C_j,p) = 2$ if $i \neq j$. If $R(C_1,p) \cap R(C_2p) \cap R(C_3,p) = \{0\}$ then

$$\dim ((R(C_1,p) \cap R(C_2p)) + (R(C_1,p) \cap R(C_3,p) = 4.$$

Let T_1, T_2 be a basis of $R(C_1,p) \cap R(C_2,p)$, T_3, T_4 be a basis of $R(C_1,p) \cap R(C_3,p)$ and T_5, T_6 be a basis of $R(C_2,p) \cap R(C_3,p)$ mod p. Evidently, for s and t any of 1 to 6, we can write $T_s \equiv X_s\ C_i(p)$ and $T_r \equiv X_r\ C_i(p)$ for some X_s and X_r and we therefore have that $(T_s, T_r) \equiv (X_s\ C_i, X_r\ C_i) \equiv (X_s, X_r)\ N(C_i) \equiv 0(p)$. By symmetry, we may assume that $T_s = T_1$ and we then have T_1, T_2, T_3, T_4 as multiplies of C_1 and T_1, T_5, T_6 as multiplies of C_2 mod p. Now since $(T_s, T_r) \equiv 0(p)$ $(s,r = 1,2,3)$, and $\dim((R(C_1,p) \cap R(C_2,p)) + (R(C_1,p) \cap R(C_3,p)) = 4$, we have $\dim \{x_1 T_1 + \ldots + x_6 T_6\}_p = 4$ because this last space is isotropic. Therefore $T_5 \equiv a_1 T_1 + \ldots + a_4T_4(p)$ from which it follows that $T_5 \overline{C}_1 \equiv 0(p)$ since $T_i \overline{C}_i \equiv 0(p)$ $(i = 1,2,3,4)$. We also have $T_5 \overline{C}_2 \equiv T_5 \overline{C}_3 \equiv 0(p)$. Since T_5 is in $R(C_2p) \cap R(C_3p)$. By lemma 1 $0 \not\equiv T_s \equiv X_1 C_1 \equiv X_2 C_2 \equiv X_3 C_3(p)$ for some X_1, X_2, X_3 or

T_5 is in $R(C_1p) \cap R(C_2p) \cap R(C_3,p)$ which is a contradiction, and dim $(R(C_1,p) \cap R(C_2,p) \cap R(C_3,p)) > 0$. If A and B, $A \not\equiv 0 \not\equiv B(p)$ have residues in $R(C_1,p) \cap R(C_2,p) \cap R(C_3,p)$ then $A \equiv X_i\ C_i(p)$ and we have $A\overline{C}_i \equiv B\overline{C}_i \equiv 0(p)$ or $C_i\overline{A} \equiv C_i\ \overline{B} \equiv 0(p)$ which implies, by lemma 1, that C_1, C_2, C_3 are all elements of $R(A,p) \cap R(B,p)$ mod p. This implies by lemma 2, that dim $(R(A,p) \cap R(B,p)) = 4$ and we therefore have $A \equiv tB(p)$ for some t.

Since $A\overline{C} \equiv 0(p)$, $N(C) = p$ is equivalent to $A = A'C$, $N(C) = p$. Hence this lemma says that, given three integral Cayley numbers C_1, C_2, C_3 which are linearly independent mod p, mutually orthogonal and of norm p, there are uniquely determined Cayley numbers A and B of which the given three are right divisors and left divisors respectively. Thus, if $N(A) \equiv 0(p)$, $A \not\equiv 0(p)$, then three right (or three left) divisors of A of norm p uniquely determine the remaining right (or left) divisors of norm p. We will return to this point later.

Lemma 4 If $C_1, \ldots, C_8$ are such that $(C_i\ C_j) = p\ \delta_{ij}$ $(i,j = 1, \ldots, 8)$ then $C_1, \ldots, C_8$ generate a four dimensional space mod p.

Proof: Since $(C_i, C_j) \equiv 0(p)$, dim $\{x_1\ C_1 + \ldots + x_8\ C_8\} \underset{p}{\leq} 4$.

Now $X \equiv x_1\ C_1 + \ldots + x_8\ C_8(p)$ if and only if $(X, C_i) \equiv 0(p)$

for each i. For $X \equiv x_1 C_1 + x_8 C_8 (p)$ implies $(X, C_i) \equiv 0(p)$ for each i. Conversely we have for any X in ζ, $X = x_1 C_1 + \ldots + x_8 C_8$ (x_i rational, i = 1, ... , 8). For the condition $(C_i C_j) = p \delta_{ij}$ implies that $C_1, \ldots C_8$ form a basis of the vector space $\{x_1 C_1 + \ldots + x_8 C_8 | x_i$ rational$\}$. Now $(X, C_i) = x_i p$ and $(X, C_i) \equiv 0(p)$ implies that x_i is integral (i = 1, ...,8). Therefore the dimension, d, of $\{x_1 C_1 + x_8 C_8\}_p$ equals the number of linearly independent solutions of $(X, C_i) \equiv 0(p)$, (i = 1,...8). But the rank of this system equals the dimension of $\{x_1 C_1 + \ldots + x_8 C_8\}_p$ and is therefore less than or equal to four, which implies that the dimension in question is exactly four.

Corollary If $N(A) \equiv N(B) \equiv 0(p)$, and A and B are primitive mod p, then A and B have the same right divisors of norm p if and only if $A \equiv tB$ for some t. The same statement holds regarding left divisors.

Proof The condition is sufficient since $A = tB + pK$ and $B = B'C$ with $N(C) = p$ imply that $A = (tB' + K\overline{C})C$. We also have $B = sA + pT$, since $t \not\equiv 0(p)$ and $A = A'C$, $N(C) = p$, implies $B = (sA' + T\overline{C})C$. Necessity follows from lemmas 3 and 4 since both A and B then have three linearly independent right or three linearly independent

left divisors of norm p in common

Lemma 5 If C_1, C_2, C_3 are linearly independent mod p and if $(C_i, C_j) \equiv 0(p)$ $(i,j = 1,2,3)$, then there are two distinct subspaces of ζ_p which contain residues mod p of C_1, C_2 and C_3, are isotropic and are maximal with respect to the last two properties.

Proof By lemma 3 there is an A, $A \not\equiv 0(p)$, such that $A\overline{C}_i \equiv 0(p)$ or $A \equiv X_i C_i(p)$ for some $X_i (i = 1,2,3)$. Now $N(A) \equiv 0(p)$ and $R(A,p)$ is a maximal isotropic subspace containing the residues, mod p, of C_1, C_2, C_3. Let $(C_1, C_2, C_3, C_4)_p = R(A,p)$. ζ_p may now be expressed as $(C_1, B_1)_p \perp (C_2, B_2)_p \perp (C_3, B_3)_p \perp (C_4, B_4)_p$, where $N(B_i) \equiv 0(p)$ and $(C_i, B_i) \not\equiv 0(p)$ $(i = 1,2,3,4)$. Suppose C_1, C_2, C_3, C form a basis, mod p, of a second maximal isotropic space. Then, mod p, C is an element of the orthogonal complement of $(C_1, C_2, C_3)_p$ which is $(C_1)_p \perp (C_2)_p \perp (C_3)_p \perp (C_4, B_4)_p$. Thus $C \equiv xC_1 + yC_2 + zC_3 + aC_4 + bB(p)$ and $N(C) \equiv 2ab(C_4,B) \equiv 0(p)$ which implies that $a \equiv 0(p)$ or $b \equiv 0(p)$ but not both. Hence $(C_1, C_2, C_3, C)_p$ must be either $(C_1, C_2, C_3, C_4)_p$ or $(C_1, C_2, C_3, B)_p$ and since these two spaces are different this also shows that there are exactly two spaces of the type mentioned.

Lemma 6 If $N(A) \equiv N(B) \equiv 0(p)$, A and B primitive mod p, then dim $R(A,p) \cap L(B,p) < 4$.

Proof Write $A = A_1 + A_2 v$ and $B = B_1 + B_2 v$ where we may assume, as in lemma 2, that $N(A_1) \not\equiv 0(p)$. If we assume $R(A,p) = L(B,p)$ and that $C_1, \ldots, C_8$ are the right divisors of A of norm p then they are also the left divisors of norm p of B, since $C \equiv XA \equiv BY(p)$ with $N(C) = p$ is equivalent to $C\overline{A} \equiv \overline{B}C \equiv 0(p)$ or $A\overline{C} \equiv \overline{C}B \equiv 0(p)$. Thus $A = A'C$ and $B = CB'$ for some A' and B'. If $C = C_1 + C_2 v$ we have

$$A\overline{C} = (A_1 + A_2 v)(\overline{C}_1 - C_2 v) = (A_1 \overline{C}_1 + \overline{C}_2 A_2) + (A_2 C_1 - C_2 A_1)v$$

and

$$\overline{C}B = (\overline{C}_1 - C_2 v)(B_1 + B_2 v) = (\overline{C}_1 B_1 + \overline{B}_2 C_2) + (B_2 \overline{C}_1 - C_2 \overline{B}_1)v.$$

Now $A\overline{C} \equiv 0(p)$ is equivalent to $C_1 \equiv -h\overline{A}_2 C_2 A_1 (p)$ where $N(A_1)\, h \equiv 1(p)$. If also $\overline{C}B \equiv 0(p)$ then we must have $\overline{B}_1 C_1 + \overline{C}_2 B_2 \equiv 0(p)$. Upon substituting $C_1 \equiv -h\overline{A}_2 C_2 A_1 (p)$ into the last congruence we obtain $-h\overline{B}_1 \overline{A}_2 C_2 A_1 + \overline{C}_2 B_2 \equiv 0(p)$, which is equivalent to $-\overline{B}_1 \overline{A}_2 C_2 + \overline{C}_2 B_2 \overline{A}_1 \equiv 0(p)$ or $(-\overline{B}_1 \overline{A}_2) C_2 \equiv \overline{C}_2 (B_2 \overline{A}_1 (p)$. The assumption that $R(A,p) = L(B,p)$ together with lemma 4 now imply that the congruence $(-\overline{B}_1 \overline{A}_2) X \equiv \overline{X} (B_2 \overline{A}_1)(p)$ holds for all X in $\mathcal{L}$.

If A' and B' are in $\mathcal{L}$ then $A'X \equiv \overline{X}B'(p)$ holds for every X in $\mathcal{L}$ if and only if $A' \equiv B' \equiv 0(p)$. This is

easily seen by substituting for X the quantities $1, i, j$ and k. Applied to our conguence this gives $\overline{B}_1 \overline{A}_2 \equiv B_2 \overline{A}_1 \equiv 0(p)$, which implies that $B_1 \equiv B_2 \equiv 0(p)$ and therefore $B \equiv 0(p)$. This contradicts the primitivity of B.

Lemma 7 If $N(A) \equiv N(B) \equiv 0(p)$, A and B primitive mod p then dim $R(A,p) \cap L(B,p) > 0$.

Proof Suppose dim $R(A,p) \cap L(B,p) = 0$ Then we could write $\mathcal{C}_p = R(A,p) \oplus L(B,p)$ and since (BA), mod p, is an element of the intersection in question we must have $BA \equiv 0(p)$. Now given X we have $B(XA) - (BX)A = (XB)A - X(BA)$ or $B(XA) \equiv (BX + XB)\, A(p)$ which implies, by our assumption, that $B(XA) \equiv 0(p)$. From this last fact and lemma 1 it follows that given X there is Y such that $XA \equiv \overline{B}Y(p)$. But this implies that $R(A,p) \subset L(\overline{B},p)$. Thus $R(A,p) = L(\overline{B},p)$, which is impossible by the preceding lemma.

Lemma 8 If M is a maximal isotropic subspace of $\mathcal{C}_p$ then there is an A in $\mathcal{C}$, $A \not\equiv 0(p)$ such that $M = R(A,p)$ or $M = L(A,p)$.

Proof By lemma 5 we know that dim $M = 4$. Let C_1, C_2, C_3, C_4 be a basis of M mod p. By lemma 3 there is an A and a B such that $A\overline{C}_i \equiv 0(p)$ and $\overline{C}_i B \equiv 0(p) (i = 1,2,3)$. Since $C_i \overline{A} \equiv 0(p)$ and $\overline{B}C_i \equiv 0(p)$ we have C_1, C_2 and C_3, mod p, in M, $R(A,p)$ and $L(B,p)$. By lemma 5 two of these spaces

must coincide, but by lemma 6 it cannot be the last two. M must therefore coincide with one of $R(A,p)$ or $L(B,p)$.

Lemma 9 If C_1, C_2, C_3, C_4 are linearly independent mod p and satisfy $(C_i, C_j) \equiv 0(p^r)(r \geq 1\ i,j = 1,2,3,4)$ then there is an A in ζ, $A \not\equiv 0(p)$, such that $A\overline{C}_i \equiv 0(p^r)$ or $\overline{C}_i A \equiv 0(p^r)(i = 1,2,3,4.)$

Proof We proceed by induction on r. The lemma is true for $r = 1$ by lemmas 5 and 8. Assuming the lemma for r we suppose that $(C_i, C_j) \equiv 0(p^{r+1})(i,j = 1,2,3,4)$. Since $(C_i, C_j) \equiv 0(p^r)$ we may find an A, $A \not\equiv 0(p)$, so that, let us say $A\overline{C}_i \equiv 0(p^r)$. By lemma 1 we have $A = X_i\ C_i(p^r)$ for some X_i and therefore $N(A) \equiv 0(p^r)$. If we choose A' such that $(A, A') \not\equiv 0(p)$, as we may, then $N(A + p^r A') = N(A) + 2p^r(A, A') + p^{2r}N(A')$ is zero mod p^r, and non zero mod p^{r+1} if $N(A) \equiv 0\ (p^{r+1})$. Since $A \equiv A + p^r A'(p^r)$ we may replace A by $A + p^r A'$, if necessary, and assume that $A\overline{C}_i \equiv 0\ (p^r)$, $N(A) \equiv 0(p^r)$ but $N(A) \not\equiv 0(p^{r+1})$.

Now set $A\overline{C}_i = p^r K_i$. In order to solve $(A + p^r B)\ \overline{C}_i \equiv 0(p^{r+1})$ for B it is necessary and sufficient that $K_i + B\overline{C}_i \equiv 0(p)$ be solvable for B. We now show that this is possible. From $p^{2r}(K_i, K_j) = N(A)(\overline{C}_i, \overline{C}_j) = N(A)\ (C_i\ C_j) \equiv 0\ (p^{2r+1})$ we have

$(K_1, K_j) \equiv O(p)$. The numbers K_1, K_2, K_3, K_4 are linearly independent mod p, for $x_1K_1 + \ldots + x_4K_4 \equiv O(p)$ implies that $x_1p^rK_1 + \ldots + x_1p^rK_4 \equiv O(p^{r+1})$ and therefore that $A(x_1\overline{C}_1 + \ldots + x_4\overline{C}_4 \equiv) O(p^{r+1})$, which in turn implies that $x_1\overline{C}_1 + \ldots + x_4\overline{C}_4 \equiv O(p)$ or $x_1C_1 + \ldots + x_4C_4 \equiv O(p)$. Thus $x_i \equiv O(p)$. By lemma 8 we know that there is a D in $\mathfrak{C}$ with $N(D) \equiv O(p)$ and $D \not\equiv O(p)$ such that $(K_1, K_2, K_3, K_4)_p = R(D,p)$ or to $L(D,p)$. We will now exclude the first possibility. Let $N(A) = mp^r$ $(m,p) = 1$ and choose n such that $nm \equiv 1(p)$. Then from $A\overline{C}_i = p^rK_i$ we have $\overline{C}_i \equiv n\overline{A}K_i(p)$. If $x_1K_1 + \ldots + x_4K_4 \equiv AX(p)$ we would have, upon multiplying through by $n\overline{A}$, $x_1\overline{C}_1 + \ldots + x_4C_4 \equiv O(p)$ in which case $x_i \equiv O(p)$. We conclude that $(K_1, K_2, K_3, K_4)_p \cap L(A,p) = \{0\}$ which is impossible, on the basis of lemma 7, if $(K_1, K_2, K_3, K_4)_p = R(D,p)$. We have also shown that $L(D,p) \cap L(A,p) = \{0\}$ from which it follows that $(\overline{D},\overline{A}) = (D,A) \not\equiv O(p)$, by lemma 2. If we now set $E = -(n\overline{A} + \overline{D})$ we have $EK_i = -n\overline{A}K_i - \overline{D}K_i \equiv -\overline{C}_i(p)$ since the residue mod p of K_i is in $L(D,p)$, and $N(E) \equiv -2n(\overline{A}, \overline{D}) \not\equiv O(p)$. Choose e so that $eN(E) \equiv 1(p)$ and set $B = e\overline{E}$. We now have $EK_i + \overline{C}_i \equiv O(p)$ or $N(E)K_i + \overline{E}\overline{C}_i \equiv O(p)$. Finally $K_i + B\overline{C}_i \equiv O(p)$. This

completes the proof of the lemma.

Lemma 10 If C_1, C_2, C_3 are linearly independent mod p and satisfy $(C_i\ C_j) \equiv O(p^r)$ $(r \geq 1 \quad i,j = 1,2,3)$ then there exist A_1 and A_2, primitive mod p, such that $A_1\overline{C}_2 \equiv O(p)^r$ and $\overline{C}_i A_2 \equiv O(p)^r$ $(i = 1,2,3)$. If B_1 and B_2 satisfy these congruences and are primitive mod p then $B_k \equiv t_k A_k (p)^r$ for some t_k $(k = 1,2)$.

Proof We shall show that there is an A, $A \not\equiv O(p)$, which is unique mod p^r, such that $A\overline{C}_i \equiv O(p^r)$ the other result following by conjugation. We begin by proving the following. Given A, C_1C_2, C_3 such that 1) C_1, C_2, C_3 are linearly independent mod p, 2) $(C_i, C_j) \equiv O(p^r)$, 3) $A\overline{C}_i \equiv O(p)$ there exists C such that 1) C, C_1, C_2, C_3 are linearly independent mod p, 2) $N(C) \equiv O(p^r)$, 3) $(C,C_i) \equiv O(p^r)$ and 4) $A\overline{C} \equiv O(p)$. That this is true for $r = 1$ follows from Theorem 1 of Chapter 1. Assuming the statement for r we suppose $(C_i,C_j) \equiv O(p^{r+1})$ along with 1.) and 3.) from which is follows (by induction) that C satisfies 1.) and 4.) of the conclusion $N(C) \equiv O(p^r)$, and $(C,C_i) \equiv O(p^r)$. Set $T = C + p^rC'$, C' to be determined. Now T, C_1, C_2, C_3 are linearly independent mod p and $A\overline{T} \equiv O(p)$ for any C'. Also $N(T) \equiv N(C) + 2p^r(C',C)(p^{r+1})$ and

$(T,C_i) \equiv (C,C_i) + p^r.(C', C_i)(p^{r+1})$. If we set $N(C) = tp^r$ and $(C,C_i) = t_ip^r$ then $N(T) \equiv O(p^{r+1})$ and $(C_i,T) \equiv O(p^{r+1})$ if and only if $t + 2(C',C) \equiv O(p)$ and $t_i + (C', C_i) \equiv O(p)(i = 1,2,3)$ has a solution for C'. That this is the case follows from the fact that C, C_1, C_2, C_3 are linearly independent mod p.

We now prove the original lemma by induction and notice that it is true for $r = 1$ by lemma 3. Assuming the lemma for r we suppose that $(C_i, C_j) \equiv O(p^{r+1})(i,j = 1,2,3)$. By induction there is A such that $A\overline{C}_i \equiv O(p^r)$. We may now find C_4 such that C_1, C_2, C_3, C_4 are linearly independent mod p, $(C_i, C_j) \equiv O(p^{r+1})(i,j = 1,2,3,4)$ $A\overline{C}_4 \equiv O(p)$. By lemma 9 then is B, $B \not\equiv O(p)$, such that either $B\overline{C}_i \equiv O(p^{r+1})$ or $\overline{C}_iB \equiv O(p^{r+1})$. If $\overline{C}_iB \equiv O(p^{r+1})$ $(i = 1,2,3,4)$ we would have $\overline{C}_iB \equiv O(p)$ and $A\overline{C}_i \equiv O(p)$ which implies $L(B,p) = R(A,p)$. This is impossible by lemma 6. Therefore $B\overline{C}_i \equiv O(p^{r+1})(i = 1,2,3,4)$ and thus $B\overline{C}_i \equiv O(p^{r+1})(i = 1,2,3)$.

Suppose now that $A_1\overline{C}_i \equiv A_2\overline{C}_i \equiv O(p^{r+1})(i = 1,2,3)$. Then $A_1 \equiv tA_2 + p^rK(p^{r+1})$, from which it follows that $K\overline{C}_i \equiv O(p)$, and thus $K \equiv sA_2(p)$ or $p^rK \equiv sp^rA_2(p^{r+1})$. Finally $A_1 \equiv (t + sp^r)\, A_2(p^{r+1})$.

Lemma 11 If an integral matrix M of order eight satisfies the congruence $M'M = p^r I$ and has rank 4, mod p, then there is A, $A \not\equiv O(p)$, with $N(A) \equiv O(p^r)$ such that M is a right or a left divisor matrix of A.

Proof Let C_1, C_2, C_3, C_4 be the Cayley numbers formed from the entries of four columns which are linearly independent mod p. Now if C is another such Cayley number then $x_1C_1 + \ldots + x_1C_4 \equiv C(p)$. This implies that $C \equiv t_1C_1 + \ldots + t_rC_4(p^r)$ for some t_i. To show this suppose $C \equiv t_1C_1 + \ldots t_4C_4(p^k)$ $k < r$. Then $C \equiv t_1C_1 + \ldots + t_4C_4 + p^kK(p^{k+1})$ and upon taking the inner product of each side with C_i $(i = 1,2,3,4)$ we have $(K, C_i) \equiv O(p)$ which implies $K \equiv z_1C_1 + \ldots + z_4C_4(p)$ since the orthogonal complement of maximal isotropic space is the space itself. Thus we have $C \equiv (t_1 + p^kz_1)\, C_1 + \ldots + (t_4 + p^kz_4)\, C_4(p^{k+1})$. By lemma 9 it is possible to find A, $A \not\equiv O$ $N(A) \equiv O(p^r)$, such that $A\overline{C}_i \equiv O(p^r)$ or $\overline{C}_iA \equiv O(p^r)$ and therefore $A\overline{C} \equiv t_1A\overline{C}_1 + \ldots + tA\overline{C}_4 \equiv O(p^r)$ or $\overline{C}A \equiv t_1\overline{C}_1A + \ldots + t_4\overline{C}_4 \equiv O(p^r)$. Since $N(C) = p^r$, we have from $\overline{C}A \equiv O(p^r)$ or $A\overline{C} \equiv O(p^r)$ that $A = BC$ or $A = CB$ for some B.

Note: By lemma 4 the rank condition for $r = 1$ is unnecessary.

In what follows, V and W, will denote integral matrices of order four which satisfy $V'V \equiv W'W \equiv -I(p^e)$ (the prime denoting transpose). U and T will denote integral matrices of order eight which have determinant ± 1. P and Q will denote permutation matrices of order eight. The equation $M = [V]\,U$ will replace

$$M = \begin{bmatrix} p^e I & V \\ O & I \end{bmatrix} U$$

where I is the unit matrix of order four.

Lemma 12 If M is an integral matrix of rank four, mod p, and which satisfies $M'M = p^e I$, then there exist P, V, and U such that $PM = [V]\,U$.

Proof This follows from the last lemma and the fact that every divisor matrix can be so represented. In fact P may be chosen so that the permutation it gives rise to on the basal elements of $\mathfrak{C}$ is an automorphism.

Lemma 13 If $M = [V]\,U = [W]\,T$, $M'M = p^e I$ then $V \equiv W(p^e)$

Proof $p^e I = M'M = T'[W][V]\,U$. Thus

$$p^e (T')^{-1}\, U^{-1} = [W]'\,[V] = \begin{bmatrix} p^{2e} I & p^e V \\ p^e W' & W'V + I \end{bmatrix}$$

Therefore $W'V + I \equiv O(p^e)$ and $W(W'V + I) \equiv -V + W \equiv O(p^e)$

Theorem 1 Let M satisfy the hypotheses of lemma 12. If $PM = [V]\,U$, $QM = [W]\,T$, for some P, Q, U, T, V, and W, then $|P| \cdot |V| \equiv |Q| \cdot |W| \ (p^e)$. Since $|P| \cdot |V| \equiv \pm 1 \ (p^e)$ the sign, mod p^e, of $|P| \cdot |V|$ is an invariant for M and will be denoted by $s(M)$.

Proof We will first prove the following statement. If $M = [V]\,U$ and $QM = [W]\,T$ then $|Q| \cdot |W| \equiv |V| \ (p^e)$.

A matrix of the form

$$\begin{bmatrix} Q_1 & 0 \\ 0 & Q_2 \end{bmatrix}$$

where Q_1 and Q_2 are permutation matrices of order four, will be called a special permutation. Q_{ij} will denote the matrix obtained from the identity matrix by interchanging rows i and j where $1 \leq i \leq 4$ and $5 \leq j \leq 8$. We will now prove the above statement where Q is a special permutation or a Q_{ij}. Suppose first that Q is a special permutation. Then

$$QM = \begin{bmatrix} p^e Q_1 & Q_1 V \\ 0 & Q_2 \end{bmatrix} U = \begin{bmatrix} p^e I & Q_1 V Q_2^{-1} \\ 0 & I \end{bmatrix} \begin{bmatrix} Q_1 & 0 \\ 0 & Q_2 \end{bmatrix} U$$

By lemma 13 $|W| \equiv |Q_1 V\, Q_2^{-1}| = |Q| \cdot |V| \ (p^e)$. Now suppose that Q is a Q_{ij}. From the equation $Q_{ij} M = Q_{ij}[V]\,U = [W]\,T$ we conclude that the last four

rows of $Q_{ij}[V]$ are linearly independent mod p, since this is the case for $[W]T$. This implies that $(v_{ik}, p) = 1$ where $k = j - 4$. Now choose x and y such that $xv_{ik} + yp^e = 1$. Let S be the matrix of order eight which differs from the identity matrix only in the ii, ij, ji, and jj positions where we have v_{ik}, y, $-p^e$ and x respectively. In what follows we will take $i = 2$ and $j = 6$ since this case is illustrative of the general case. Now $|S| = 1$ and we may write $Q_{ij}M = Q_{ij}[V]T = HS^{-1}T$ where

$$H = \begin{bmatrix} p^e & -p^e v_{12} & 0 & 0 & v_{11} & xv_{12} & v_{13} & v_{14} \\ 0 & -p^e & 0 & 0 & 0 & x & 0 & 0 \\ 0 & -p^e v_{12} & p^e & 0 & v_{31} & xv_{32} & v_{33} & v_{34} \\ 0 & -p^e v_{42} & 0 & p^e & v_{41} & xv_{42} & v_{43} & v_{44} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & v_{21} & 1 & v_{23} & v_{24} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

By performing elementary column operations on H we finally obtain $Q_{26}M = [V_1]U_1$ where

$$V_1 = \begin{bmatrix} v_{11} - xv_{12}v_{21} & xv_{12} & v_{13} - xv_{12}v_{23} & v_{14} - xv_{12}v_{24} \\ -xv_{21} & x & -xv_{23} & -xv_{24} \\ v_{31} - xv_{32}v_{21} & xv_{32} & v_{33} - xv_{32}v_{23} & v_{34} - xv_{32}v_{24} \\ v_{41} - xv_{42}v_{21} & xv_{42} & v_{43} - xv_{42}v_{23} & v_{44} - xv_{42}v_{24} \end{bmatrix}$$

The matrix

$$V_2 = \begin{bmatrix} v_{11} & xv_{12} & v_{13} & v_{14} \\ 0 & x & 0 & 0 \\ v_{31} & xv_{32} & v_{33} & v_{34} \\ v_{41} & xv_{42} & v_{43} & v_{44} \end{bmatrix}$$

has the same determinant as V_1. Using $V'V \equiv -I(p^e)$ we have

$$|V_1||V'| = |V_2||V'| \equiv x \det \begin{bmatrix} -1 & 0 & 0 & 0 \\ v_{12} & v_{22} & v_{32} & v_{42} \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = xv_{12} \equiv -1(p^e)$$

Thus $|W| \equiv |V_1| \equiv |V_2| \equiv -|V| \equiv |Q_{26}||V| \ (p^e)$

To return to the general case of an arbitrary permutation matrix Q we distinguish five cases. QM has either 0, 1, 2, 3, 4 of the last four rows of M among its first four rows. The first cas has already been considered since Q is, in that case, a special permutation. Assuming the lemma for case t $(1 \leq t < 5)$ suppose we have $M = [v]T$ and $QM = [W]U$ where QM is of case $t+1$. Consider now two sets of rows numbered as they are in PM.

1) those rows taken from the last four rows of PM which were among the first four rows of M and

2) those rows taken from the first four rows of PM which were among the last four rows of M.

Fix a row, say the j^{th}, from set 1). Then one among the elements $w_{j-4,k}$ is prime to p, where k is the number of a row in set 2). For in the contrary case interchanging, in QM, the rows of sets 1) and 2) given a matrix PM in which the last four rows are linearly independent mod p. But this happens for PM if and only if it happens for M, since P is a special permutation. However the last four rows of M are linearly independent mod p because $M = [V]T$. Thus, by the same method that was used before, there is W_1 and T_1 such that $Q_{jk}(QM) = [W_1]T_1$. The case considered for Q_{jk} gives $|W| \equiv |Q_{jk}||W_1|$. We also have $(Q_{jk}Q)M = [W_1]T$ where $(Q_{jk}Q)M$ is matrix of case t. Therefore $|Q_{jk}Q||W_1| \equiv |V|(p^e)$. Finally $|V| \equiv |Q||W|(p^e)$.

If we now have $PM = [V]U$ and $QM = [W]T_2$ then $(PQ^{-1})[W]T = [V]U$. Applying what has been proved already we see that $|PQ^{-1}| \cdot |V| \equiv |W|(p^e)$ or $|Q| \cdot |W| \equiv |P| \cdot |V|(p^e)$.

Lemma 14 Let M be an integral matrix with $M'M = mI$, m odd. If $p^e||m$, and if the rank of M is four mod p then there exist integral matrices, M_p and U such that $M_p' M_p = p^e I$ and $M = M_p U$. Furthermore M_p is unique up to equivalence.

Proof If $C_1, \ldots, C_8$ are the Cayley numbers whose coefficients are the columns of M then $(C_i, C_j) \equiv 0(p^e)$.

By lemma 9 then exists a Cayley number A_p such that $A_p\overline{C}_i \equiv 0(p^e)$ or $\overline{C}_i A_p \equiv 0(p^e)(i = 1,\ldots, 8)$. Suppose $A_p\overline{C}_i \equiv 0(p^e)$. Since $N(A_p) \equiv N(A_p) \equiv 0(p^e)$ we may find for A_p a right divisor matrix of norm p^e. Let M_p be such a matrix and let the right divisors of A_p, corresponding to M_p, be $C_1', \ldots, C_8'$. We then have $C_i \equiv x_i A_p$ and $C_i' \equiv Y_i A_p(p^e)$. From this it follows that $(C_i, C_j') \equiv 0(p^e)$ $(i,j = 1,\ldots 8)$. Thus each C_i is a linear combination mod p^e of the C_i', by an argument similar to that of lemma 11. Hence there is an integral matrix N such that $M \equiv M_p N(p^e)$. From this it follows that $M_p' M = p^e U$ or $M = M_p U$. If $M = N_p T$ then $M_p = N_p(TU^{-1})$. But $M_p' M_p = p^e I = p^e(TU^{-1})'(TU^{-1})$ or $(TU^{-1})'(TU) = I$. Hence TU^{-1} is a permutation matrix.

Note: We could have written $M_p \equiv MT(p^e)$ just as well. Since each C_i' is a linear combination of the C_i mod p^e.

Lemma 15 Let M be an integral matrix satisfying $M'M = p^e I$, and $PM = [v]U$ for some P, V, and U. Then M is a right or a left divisor matrix according as $|P| \cdot |V| \equiv 1\,(p^e)$ or $|P| \cdot |V| \equiv -1\,(p^e)$.

Proof Suppose M is a right (left) divisor matrix for $A = A_1 + A_2 v$, A_i in $\mathfrak{L}$. By applying an automophism to

we may secure $N(A_1) \not\equiv 0(p)$. M is then changed to QM where QM is a right (left) divisor matrix, and $|Q| = 1$. Let $X = x_0 + x_1 i + x_2 j + x_3 k$ and $Y = y_0 + y_1 i + y_2 j + y_3 k$. Denote by (x) and (y) the column vectors formed from the components of X and Y respectively. By the computations carried out in chapter 1 we have

$QM = [W]U$ where

$(y) \equiv W(x)(p^e)$ is equivalent to $Y \equiv -h\overline{A}_2 XA_1(p^e)$ in case M is a right divisor matrix or

$(y) \equiv W(x)(p^e)$ is equivalent to $Y \equiv -hA_1 \overline{X}A_2(p^e)$ is case M is a left divisor matrix ($hN(A_1) \equiv 1(p^e)$). Hence $|W|$ is equal to the determinant of the transformation $X \to h\overline{A}_2 XA_1$ or $X \to -hA, \overline{X}A_2$, mod p^e. If $B \in \mathfrak{L}$, simple calculations show that the determinants of the transformations $X \to XB$, $X \to BX$, and $X \to \overline{X}B$ are $N(B)^2$, $N(B)^2$, and $-N(B)^2$ respectively. Using the fact that $h^2N(A_1)\ N(A_2) \equiv -1(p^e)$ we have that QM is a right or left divisor matrix according as $|W| \equiv 1$ or $-1(p^e)$. But $|P| \cdot |V| \equiv |Q| \cdot |W| \equiv |W|\ (p^e)$.

<u>Theorem 2</u> Let $m = {p_1}^{e} \ldots {p_n}^{en}$ be an odd positive integer. Let M be an integral matrix which has rank four mod p_i ($i = 1, \ldots, n$), and which satisfies $M'M = mI$. If $M = M_{p_i} U_i$, where U_i and M_{p_i} are determined by lemma 14,

then a necessary and sufficient condition that M be a divisor matrix is that $s(M_{p_1}) = s(M_{p_2}) = \ldots = s(M_{p_n})$

Furthermore M is a right or a left divisor matrix according as the common sign is 1 or -1.

Proof Suppose $s(M_{p_1}) = \ldots = s(M_{p_n})$. Let A_{p_i} be the Cayley number of which M_{p_i} is a divisor matrix. Then the equality among the $s(M_{p_i})$ insures that the M_{p_i} are either all right or all left divisor matrices (we will suppose they are all right divisor matrices). By the Chinese Remainder Theorem find A such that $A \equiv A_{p_i}(p^{e_i})(i = 1,\ldots, n)$ If $C_1, \ldots, C_8$ are the Cayley numbers associated with M then we know that $A\overline{C}_i \equiv A_{p_i}\overline{C}_i \equiv O(p^{e_j})(i = 1,\ldots,8\ j = 1,\ldots,n)$ Thus $A\overline{C}_i \equiv O(m)$ and the C_i are right divisors of A, of norm m.

Conversely, suppose M is a right divisor matrix of A and that $M = M_{p_i} U_i$. By the note at the end of lemma 14 write $M_{p_i} \equiv MT_i(p_i^{e_i})$. If $C_1, \ldots, C_8$ are the Cayley numbers associated with M_{p_i}, it follows from the last congruence that $A\overline{C}_j \equiv O(p_i^{e_i})$. For the columns of M_{p_i} are linear combinations, mod $p_i^{e_i}$, of the columns of M. Hence each M_{p_i} is a right divisor matrix and the theorem

follows by lemma 15.

Theorem 3 If M is a divisor matrix of norm m (modd) define $s(M) = 1$ or -1 according as M is a right or left divisor matrix. If P is a permutation matrix then PM is a divisor matrix and $s(PM) = |P|\ s(M)$.

Proof If $p^e||m$ and $M = M_p U$ $(M_p' M_p = p^e I)$ then $PM = (PM_p)\ U$ and our theorem follows from theorem 3 and lemma 15.

Given an odd positive integer m we now answer the following two questions. 1) If $N(A) \equiv N(B) \equiv 0(m)$, A and B, primitive mod m, when do A and B have the same set of right (left) divisors of norm m? 2) How many right left divisors or norm m may be specified?

Theorem 4 If $N(A) \equiv N(B) \equiv 0(m)$, A and B primitive mod m, then A and B have the same set of right (left divisors of norm m if and only if $A \equiv tB(m)$ for some t.

Proof The condition is clearly sufficient. Suppose now that A and B have the same right divisors of norm m. Let M be their common divisor matrix, and let $C_1, \ldots, C_8$ be the Cayley numbers associated with M. If $p^e||m$ we then have $A\overline{C}_i \equiv B\overline{C}_i \equiv 0(m)$ and hence $A\overline{C}_i \equiv B\overline{C}_i \equiv 0(p^e)$ $(I = 1, \ldots, 8)$. Thus, by lemma 10, $A \equiv t_p B(p^e)$. Let $t \equiv t_p(p^e)$ for each p dividing m.

Then $A \equiv tB(p^e)$ for each such p and we have $A \equiv tB(m)$.

Theorem 5 If C_1, C_2, C_3 are linearly independent mod p, for each p dividing m, and if $(C_i, C_j) = O(m)(i,j=1,2,3)$ then there exists A and B, $N(A) \equiv N(B) \equiv O(m)$, such that $A\overline{C}_i \equiv \overline{C}_i B \equiv O(m)$. If A' and B' also satisfy these conguences then $A \equiv tA'$ and $B \equiv sB'(m)$.

Proof Since $(C_i, C_j) \equiv O(p^e)(p^e||m)$ we may, by lemma 10, find A_p and B_p such that $A_p\overline{C}_i \equiv \overline{C}_i B_p \equiv O(p^e)$. If we set $A \equiv A_p(p^e)$ and $B \equiv B_p(p^e)$ (for each p) then $A\overline{C}_i \equiv \overline{C}_i B \equiv O(m)$. Suppose now that $A'\overline{C}_i \equiv O(m)$. Then, by lemma 10, $A \equiv t_p A'(p^e)$, for each p. Find t so that $t \equiv t_p(p^e)$, for each p. Then $A \equiv tA'(p^e)$, for each p, and we have $A \equiv tA(m)$.

Let C_1, C_2, C_3 be linearly independent mod p, for each p dividing m. Suppose also that $(C_i, C_j) = m\,\delta_{ij}$. Then the last theorem states that there are number A and B of which the given three are right and left divisors respectively. Furthermore A and B are uniquely determined up to scalar multiples mod m. Hence, if $N(A) \equiv O(m)$ (A primitive mod m) then the right (left) divisors of A, of norm m, are uniquely determined by any three of them satisfying the above conditions.

BIBLIOGRAPHY

1. Artin, E. Geometric Algebra. New York: Interscience Publishers, Inc., 1957.

2. Jacobson, N. "Composition Algebras and Their Automorphisms," Rendiconti del Circolo Matematico di Palermo, Serie II, Tomo VII (1958), 55-65.

3. Mordell, C. J. "The Definite Quadratic Forms in Eight Variables with Determinant Unity," Journal de Mathematiques, XVII (1938), 41-46.

4. Pall, G. "Representation by Quadratic Forms," Canadian Journal of Mathematics, Vol. I, No. IV (1949) 354-355.

VITA

Charles Julius Feaux, Jr. was born on October 30, 1935 in San Diego, California. He attended the public schools of the cities of New York, New York; Indianapolis, Indiana; and San Diego, California. In September of 1953, he entered San Diego State College, San Diego, California, where he received his B.A. degree in Mathematics in February, 1958. At that time he entered the Illinois Institute of Technology for one semester, as a graduate assistant in mathematics. He entered the University of Wisconsin in September of 1958, and spent one year as a graduate assistant in mathematics. Finally, he entered Louisiana State University as a graduate assistant and is currently a candidate for the degree of Doctor of Philosophy in the Department of Mathematics.

EXAMINATION AND THESIS REPORT

Candidate: Charles Julius Feaux, Jr.

Major Field: Mathematics

Title of Thesis: Divisor Matrices in the Cayley Ring

Approved:

Gordon Pall
Major Professor and Chairman

Max Goodrich
Dean of the Graduate School

EXAMINING COMMITTEE:

Gordon Pall

H. S. Butts

R. G. Kuch

W. Scott Cohn

L. L. Wade

Date of Examination:

July 19, 1966